Town of Granby
Computer Equipment and Services
Acceptable Use Policy

1. Introduction

The Town of Granby provides staff with computer equipment and the ability to communicate and receive information using electronic mail and the Internet. The town utilizes this technology to improve staff efficiency and communication, and to serve the public more effectively. These computer resources are the property of the Town of Granby and should be used for appropriate business purposes only. The Town reserves the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy. Town users are expected to use their access to electronic mail and the Internet in a responsible and informed way.

Questions regarding acceptable use can be referred to the Information Systems Coordinator or the Town Administrator.

2. Prohibited Activities

The following activities are strictly prohibited:

- Any illegal activity, including, but not limited to, the transmission of copyrighted or trade secret material, obscene or threatening materials, or the participation in any type of criminal activity.
- Transmission of materials used for commercial promotion, product endorsement or political lobbying.
- Attempts to violate the Town of Granby computer system or the computer system of any other municipality, institution, organization, company or individual.
- Connection of individually (non-Town) owned equipment to the Town's network **without prior authorization**.
- Software piracy, or the downloading and transferring of software for which the user does not have proper licensing.

3. Use of Computers

3.1 Authorized Use

Computers are provided for specific individuals who utilize them to perform their job functions. Department Heads are responsible for determining which personnel are authorized to use each computer under the Department Head's purview. Any unauthorized use of computer equipment is prohibited. Use of computer equipment for personnel gain is strictly prohibited.

3.2 Software

The copying or installing of software programs without prior approval of the Information Systems Coordinator or the Town Administrator is prohibited.

3.3 Virus Checking

Data files such as word processing documents; spreadsheets and database files, which originate from computers other than those located in a town office must be checked for viruses before use. Users needing procedures for checking viruses should contact the Information Systems Coordinator. The Information Systems Coordinator may impose additional restrictions or regulations on the importing of files from computers outside the Town's network. Additionally, failure to scan files for viruses may result in the individual's loss of computer privileges and may subject the individual to disciplinary action, up to and including discharge.

3.4 Storage

Documents and data files stored on the Town's computers are the property of the Town and may be accessed by authorized personnel for the purpose of, but not limited to, system maintenance, back-up, recovery, virus checking and adherence to this policy.

4. Use of Passwords

4.1 Confidentiality

Passwords should be kept confidential at all times. Users should endeavor to create passwords that are unique and not easily discoverable.

4.2 Changing Passwords

Users should periodically change their passwords. Users needing instructions for changing their password should contact the Information Systems Coordinator.

5. Use of Electronic Mail (Email)

5.1 Town Business

Email is an effective way to communicate with Town individuals and other job related contacts. Email is to be used for town business only. While Email shall not be used for personal gain or to conduct personal business, it may be used for limited personal communication subject to review and discretion of the Department Head. Email and any related on-line services are the property of the Town of Granby. Abuse of this privilege could result in the loss of electronic mail for the individual.

It is the responsibility of all Department Heads to implement the Email policy as appropriate. These procedures should: specify whether Email documents should be filed electronically or as paper; establish appropriate use of Email within this policy; establish procedures, where applicable, for providing public access to electronic files and collecting appropriate fees charged for materials; and monitor compliance with Town policy and department procedures.

It is the responsibility of the Information Systems Coordinator to support and maintain the Town's email system and provide routine backup and off-site storage of Email files for disaster recovery purposes.

5.2 Content

Electronic mail should never be used for any illegal activity, included but not limited to, the transmission of copyrighted or trade secret material, the transmission of obscene, defamatory, or threatening material, or the propagation of any type of criminal activity. Electronic mail should also never be used to create offensive or disruptive messages or images. Among those things which are considered offensive are any messages or images which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.

5.3 Public Record

The term "public records" is defined by statute to include all documentary materials or data, regardless of physical form or characteristics, made or received by an officer or employee of any agency or municipality of the Commonwealth, unless falling within a statutory exemption (M.G.L. C.4, S.7). Therefore, the Secretary of the Commonwealth advises that the Public Records Law clearly applies to government records generated or received electronically. Electronic mail is a Town of Granby resource and is provided as a business communications tool. All electronic mail sent, and all electronic mail received by principal addressees (not received as a "cc") (accordance with the current open meeting laws) at a Town-issued address, or any address when in an official capacity, should be considered a public record subject to inspection and disclosure and scheduled retention and disposition. Individuals and committee members acting in their official capacity should have no expectation of privacy in their use of electronic mail.

Email messages are considered public record and therefore are discoverable. Users are considered the custodians of their messages and should maintain messages according to relevant public record law.

5.4 Committee Use of Electronic Mail

In order to assist members of governmental bodies to comply with the Open Meeting Law in their use of this technology, the Town of Granby affirms that no substantive discussion by a quorum of members of a governmental body about public business within the jurisdiction of the governmental body is permissible except at a meeting held in compliance with the requirements of the Open Meeting Law. Like private conversations held in person or over the telephone, e-mail conversations among a quorum of members of a governmental body that relate to public business violate the Open Meeting Law, as the public is deprived of the opportunity to attend and monitor the e-mail "meeting."

Despite the convenience and speed of communication by e-mail, its use by members of a governmental body carries a high risk of violating the Open Meeting Law. Not only do private e-mail communications deprive the public of the chance contemporaneously to monitor the discussion, but also by excluding non-participating members, such communications are also inconsistent with the collegial character of governmental bodies. For these reasons, the Town of Granby cautions that e-mail messages among members of governmental bodies are best avoided except for matters of a purely housekeeping or administrative nature.

5.5 Filing and Retention

This Policy is intended to provide for efficient retention of E-mail communications. E-mail communications are considered public records and retention and disposition of public records are authorized by retention schedules issued by the Secretary of the Commonwealth. Transmission data contained in an E-mail communication (including the sender, addressee, date and time of transmission, and receipt) should be retained as part of the record, whether the record it printed out or stored electronically.

Departments may retain E-mail in hard copy, electronically, or by a combination of these two means. E-mail has to be keep for 7-years by law. E-mail should not be retained electronically for longer than two years; after that time, the record should be printed and retained in paper form. Departments are responsible for developing filing systems that include E-mail and are responsible for instructing individuals on appropriate use of these systems.

When appropriate, E-mail messages may be filed with program records and assume the same retention as the records they are filed with. When E-mail records do not relate obviously or directly to a program, they may be filed as correspondence. If a particular record is not described on an existing records retention schedule, the appropriate department head may apply to the Supervisor of Public records for authority to dispose of that record, and to add records to existing schedules. Only when E-mail messages are clearly conversational and do not add in any way to the operational records of the department, may they be discarded without adhering to retention schedules. Examples of this form of E-mail include: “Sorry I missed you via telephone. Please call me when you have a minute.”; “I will be out of the office at a conference this Thursday, so please mark your calendar.”; or “This is a reminder of this Friday’s staff meeting. Please send along any agenda items you may have.”

Some E-mail systems enable users to enclose or attach records to messages. These enclosed or attached records need to be filed according to their function and content, and they will assume the retention schedule of the records they are filed with.

5.6 Confidentiality

Email (particularly Internet email) should be viewed as an unsecured mode of communication. Confidential information should **NEVER** be sent via electronic mail. Individuals should never assume that email messages or Internet postings are personal or confidential. All messages sent or received by electronic mail can be tracked by the Town’s computer system. The Information Systems Coordinator and the Town Administrator reserve the right to monitor Email messages and to access all Email residing on the Town’s equipment or property. Individuals are not authorized to retrieve or read messages that are sent to them unless the intended recipient gives

express permission. No employee shall change any portion of a previously sent Email without authorization.

5.7 Unsolicited Email

Unsolicited email received from the Internet should not be opened. The user should delete the message immediately. Never open an attachment, especially if you do not know the source. Opening unknown attachments could initiate a virus.

6 Use of Internet Browsing Software

6.1 Privileges

Internet browsing capabilities are extended to those individuals requiring access to information on the World Wide Web. Use of the Internet by individuals is a privilege, not a right, which may be revoked at any time for inappropriate conduct. All individuals are responsible for complying with this policy. Violations may result in a revocation of Internet access privileges and any other applicable disciplinary action.

6.2 Standards of Conduct

Individuals have an obligation to use their access to the Internet in a responsible and informed way, conforming to network etiquette, customs, and courtesies. Use of the Internet encompasses many different interconnected networks and computer systems. Many of these systems are provided free of charge by universities, public service organizations and commercial companies. Each system has its own rules and limitations, and guests on these systems have an obligation to learn and abide by the rules.

Each employee using the Town's Internet facilities shall identify himself or herself honestly, accurately and completely (including one's company affiliation and function where requested) when participating in chats or newsgroups, or when setting up accounts on outside computer systems.

Only those individuals or officials who are authorized to speak to the media, to analysts or at public gathers on behalf of the Town may speak/write in the name of the Town to any newsgroup or chat room. Other individuals may participate in newsgroups or chats in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves. Where an individual participant is identified as an employee or agent of the Town, the employee must refrain from any political advocacy and must refrain from unauthorized endorsement or appearance of endorsement by the Town. Only those officials who are authorized to speak to the media, to analysts or in public gatherings on behalf of the Town may grant such authority to newsgroups or chat room participants.

The Town retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any employee in the course of his or her duties.

Individuals are reminded that chats and newsgroups and public forums where it is inappropriate to reveal confidential Town information. Individuals releasing such confidential information via a newsgroup or chat- whether or not the release is inadvertent- will be subject to disciplinary action, up to and including discharge.

6.3 Prohibited Activities

- No employee may use the Town's Internet facilities to propagate any virus, worm, Trojan horse, or trap door program code.
- No employee may use the Town's facilities to download or distribute pirated software or data.
- The display of any kind of sexually explicit image or document on any Town system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.
- The Town's Internet facilities and computing resources must not be used to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. Use of any company resources for illegal activity is grounds for immediate dismissal, and we will cooperate with any legitimate law enforcement activity.
- No employee may use the Town's Internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
- Individuals with Internet access may not use Town Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.
- Use of Town Internet access facilities to commit infractions such as misuse of Town assets or resources, sexual harassment, unauthorized public speaking and misappropriation of intellectual property are also prohibited.
- Sending chain letters.
- Use of abusive or objectionable language in either public or private messages.
- Use of official dissemination tools to distribute personal information.

6.4 Security

The Town has software and systems in place that monitor and record all Internet usage. Our security systems are capable of recording (for each and every user) each World Wide Web site visit, each chat, newsgroup or Email message, and each file transfer into and out of our internal networks, and we reserve the right to do so at any time. No employee should have any expectation of privacy as to his or her Internet usage. Our TA and IT will review Internet activity and analyze usage patterns, and they may choose to publicize this data to assure that company Internet resources are devoted to maintaining the highest levels of productivity.

The company uses independently supplied software and data to identify inappropriate or sexually explicit Internet sites. We may block access from within our networks to all such sites that we know of. If you find yourself connected accidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.

The Town has installed an Internet firewall to assure the safety and security of the company's networks. Only those Internet services and functions with documented business purposes will be enabled at the Internet firewall. Any employee who attempts to disable, defeat or circumvent any Town security facility will be subject to immediate dismissal.

6.5 Job Functions

Browsing should be limited to Internet sites directly related to the user's job function. Individuals with Internet access may not use town Internet facilities to download images or videos unless there is an express business-related use for the material.

6.6 Downloading

Individuals with Internet access may download only software with direct business use, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license. Under no circumstances should software programs be downloaded from the Internet and/or installed without prior permission of the Information Systems Coordinator or the Town Administrator. See section 3.2.

Careful consideration should be made before downloading data files (word-processing and spreadsheet files) from an Internet site. The reliability of the source of the document should be considered. Since harmful programs can be transmitted via documents, all documents must be checked for viruses prior to use. See section 3.3.

Any software or files downloaded via the Internet into the Town's network become the property of the Town. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

7 Referral to the Information Systems Coordinator

All matters relating to unusual occurrences must be reported immediately to the Information Systems Coordinator. When something unusual occurs, record information such as steps taken and warnings from the computer to aid the Information Systems Coordinator in diagnosing the situation.

8 Sanctions

Any employee who violates this policy or uses the Town's computer system for inappropriate purposes shall be subject to disciplinary action, up to and including discharge.

Town of Granby
Computer Equipment and Services Acceptable Use Policy
Confirmation of Receipt

The use of the Town's computer system constitutes individual consent to monitoring of systems and is conditioned upon strict adherence to this policy. Any individual who violates this policy or uses the Town's computer system for improper purposes shall be subject to disciplinary action, up to and including discharge.

I certify that I was given a copy of this policy and provided the opportunity to ask questions about its content.

_____
Name (printed)

_____ _____
Signature Date